IN THE CLAIMS:

1 – 58. (Canceled)

59. (Newly Added) A security gateway comprising:

a first logical interface to a first network;

a second logical interface to a second network;

a physical interface to an untrusted network through which a logical connection can be established to hosts, including hosts in a protected network; and

a processor that is configure to

- perform source network address translation (SNAT)on packets that arrive at the first logical interface which are destined to the second network or to a host coupled to the untrusted network that is outside the protected network, and to communicate the SNAT processed packets to their respective destinations,
- refuse to establish communication to a host on the first network for a device on the second network,
- perform SNAT on packets that arrive at the second logical interface and that are destined to a host on the untrusted network that is outside the protected network, and to communicate the SNAT-processed packets to their destination, and
- send via the untrusted network, by use of an IPSec tunnel, packets that arrive at the first logical interface and that are destined to the protected network.

60. (Newly Added) The apparatus of claim **59** where the processor is further configured to refuse to forward packets to the protected network from a host on the untrusted network or on the second network.

61. (Newly Added) The gateway of claim **59** where the first logical interface and the second logical interface are coupled to two distinct physical connection ports of the gateway.

62. (Newly Added) The gateway of claim **59** where the gateway is interposed between the internet and the set of the first and the second logical interfaces.

63. (Newly Added) The gateway of claim **59** where the first network and the second network are co-located

64. (Newly Added) The gateway of claim **59** where the first network comprises at least one computer and the second network comprises at least one computer.

65. (Newly Added) The gateway of claim **59** where in performing SNAT, the processor inserts into outgoing packets an IP address that belongs to the gateway.

66. (Newly Added) The gateway of claim **59** where the processor operates pursuant to modifiable stored rules that allow at least some devices in the first network to establish a connection to hosts on the untrusted network that are outside the protected network.

67. (Newly Added) The gateway of claim **59** where the processor is further configured to refuse to establish a connection to the first network for a host on the second network or on the untrusted network.

68. (Newly Added) The gateway of claim **59** where the processor is further configured to decline to perform destination network address translations (DNAT) on packets destined to the first logical interface unless a connection was first established by the packets arriving to the gateway from via the first logical interface.

69. (Newly Added) The gateway of claim **59** where the SNAT operations are performed pursuant to packet handling rules stored in the gateway.

70. (Newly Added) The gateway of claim **69** where the packet handling rules are sensitive to identity of devices of the first network, having a capability for permitting

access selected ones of the devices of the first network to gain access to a host in the untrusted network.

71. (Newly Added) The gateway of claim **59** where the processor is further configured to permit client on the untrusted network a limited access through the gateway to a server, when addressed to a preselected network port of a preselected address of the gateway, with the gateway performing destination network address translation (DNA) of the preselected port and address to the address of the server, where the preselected port and address are selected without regard to the address of the server in to which the limited access to initiate communication is granted.

72. (Newly Added) The gateway of claim **71** where the server is on the first network.

73. (Newly Added) The gateway of claim **71** where the server is on the protected network, and the passage of packets from the gateway to the server is via an IPSec tunnel.

74. (Newly Added) The gateway of claim **71** where the server is on the second network.

75. (Newly Added) The gateway of claim **59** further comprising a logical interface to a second protected network, and the processor is configured to send packets that arrive at the first logical interface which are destined to the second protected network to their destination via the untrusted network, by use of an IPSec tunnel.